TOP SECRET

1F-1531

C O P Y (Partial)

OP-20K & OP32Y
N5
NY4
NY1
S-5455

FIRST DETAILED INTERROGATION OF CARELLI Adriano

Rank:	Lieut
Unit and Function:	SIM CRYPTOGRAPHIC SECTION In Slav Group till Armistice
Interrogated:	CSDIC(Main) CMF, 20 Nov 44

Subject of Report: SIM Cryptographic work on RUSSIAN, CROAT, CETNIK and BULGARIAN traffic.

1. PREAMBLE

Source was born in LENINGRAD in 1908. His father was an Italian singing master at the Imperial Russian Court. As a child he spoke Russian fluently. The family returned to ITALY in summer 1914. Source studied law and later entered the Italian Civil Service (State Archives Department of the Ministry of the Interior). He did no cryptographic work before 1942, but on 2 Mar of that year he was drafted to SIM Crypto Section where he was wanted for his knowledge of Russian. He was first employed as a translator, under Lt. Col EMER (cf.CSDIC/CMF/Y 10), but in Sep 42 took a four months course in cryptography and at end Jan 43 began work as a cryptographer in the Slav languages group under Lt. Col SERRAGLI (cf.CSDIC/CMF/Y 4 para 5 A). He worked for both the Diplomatic and Army and Research Sub-secs. Shortly before the Italian armistice Source went to hospital because of nervous disorders, and on his discharge returned to the Ministry of the Interior.

He gave information willingly, and appeared very keen to be helpful. However, his memory is not very good, a fact which he attributes to nervous trouble of which he is a victim.

Reliability: Fairly Good

2. RUSSIAN MILITARY CODES AND CIPHERS

(a) Railway Service Code ("Codice Ferroviario")

A copy of this code had been acquired by SIM, and it was read until summer 1942, when it was replaced by another code. According to Source, though this code was originally intended to be used only by Movements Branch of the Russian Army, it was in fact used by all Q Branches, such as Supplies, Transport, Medical, etc.

It was a four-figure code, of 10,000 groups, arranged alphabetically. There were a few alternative groups; e.g. the "full stop" had three groups ("omofoni") only. The code was reciphered by means of tables. These were broken fairly easily. The tables were drawn up on the lines of the field ciphers illustrated below (sub-para b) and served to convert 2-figure bigrams into other 2-figure bigrams. Thus code-group 1453 would be reciphered to 9976, where the bigram 14 had been converted to 99 and the bigram 53 converted to 76 with the aid of the recipher table.

Traffic in this code was signalled in four-figure groups. (NOTE: Source stated that Russian military traffic was always signalled on these lines, i.e. groups of 5 symbols meant a 5 symbol code, groups of 3 a 3 symbol code, etc.)

(b) Field Codes and Field Ciphers

From Source's statements the 10x10 square field code referred to by Lt. Col EMER in CSDIC/CMF/Y 10 para 3 e iii should have been called field cipher. Present Source says that only clear letters and figures were used in the square, NOT clear words; it was in fact a two-figure bigram substitution cipher. It was used extensively in 1942. Source confirmed EMER's statement, in a/m report, that reading became impossible owing to frequent changes. See further at App "A".

Also extensively used in 1942 was a three-figure trigram substitution field code, containing clear letters, figures and words (see Appendix "A"). This code was read in 1942 (after that date Source is not certain). Considerable assistance in breaking it was given by the Hungarian Cryptographic Service (see CSDIC/CMF/Y 10, App "E") which had succeeded in reading this type of traffic first. Breaking of the different keys used for this code was further assisted by the fact that the Russians often "enciphered" words already provided in the clear part of the code by means of encoding each letter separately, rather than choosing the trigram allotted for the word concerned. This helped identification of trigrams which stood for a set of clear letters.

(see para 2 b of attached report)

1. Two-figure bigram substitution field cipher

A square of 10 x 10 small squares inside which clear letters and figures were placed according to a certain pattern. The key(s) to the encipher, i.e. the arrangement of the digits indicating the columns and the lines of the large square, were changed very often.

	6	9	3	0	4	2	8	1	5	7
0										
6										
4										
7										
1										
5										
9										
3										
8										
2										

2. Three-figure trigram substitution field code

A larger field code, containing clear words, letters and figures, and devised on the lines of the sketch below.

		2	3	9	7	4	5	0	1	6	8
	1										
	2										
	8										
	0										
	7										
1	6										
	4										
	3										
	5										
	9										
	1										
	3										
	5										
	7										
2	8										